REMARKS

The following remarks are made in response to the Office Action mailed September 2, 2004. Claims 1-59 were rejected. With this Response, claims 16 and 35 have been amended and claims 15 and 35 have been cancelled without prejudice. Claims 1-14, 16-34, and 36-59 remain pending in the application and are presented for reconsideration and allowance.

Objections to the Specification

The Examiner requested that the Applicant update the status of all parent priority applications in the first line of the specification.

Applicant has accordingly amended the specification to update the status of the Cross-Reference to Related Applications.

In view of the above, Applicant respectfully requests that the objections to the specification be removed.

Claims Rejections under 35 U.S.C. § 112

The Examiner rejected claims 15, 16, 35 and 36 under 35 U.S.C. § 112, second paragraph.

In response, dependent claims 15 and 35 have been cancelled without prejudice. Dependent claim 16 has been amended to now depend from independent claim 1 and dependent claim 36 has been amended to now depend from independent claim 21.

Therefore, Applicant respectfully requests that the rejection under 35 U.S.C. § 112, second paragraph be removed and that dependent claims 16 and 36 be allowed.

Claim Rejections under 35 U.S.C. § 102

The Examiner rejected claims 1-8, 10, 14, 15, 17-28, 30, and 35 as being anticipated by the Ramasubramani et al. U.S. Patent No. 6, 233,577.

In a public key cryptosystem, a subject (e.g., a human or a computer system) has a public/private key pair and uses the key pair to demonstrate its identity to another user of the same cryptosystem referred to as a verifier. The subject matter claimed in the pending claims relates to a subject employing a public key validation service (PKVS) to validate the subject's public key before using the public/private key pair for authentication purposes, in such a way

that the public key will cease to be usable for authentication purposes if the subject notifies the PKVS that the private key has been compromised. The PKVS includes one or more public key validation agents (PKVAs), each PKVA having a private/public key pair for a digital signature cryptosystem. In embodiments of the present invention, the subject may use its private/"validated" public key pair for multiple authentication purposes. Example authentication methods which are disclosed in the present specification which are modified to take advantage of a PKVA include: an authentication using traditional public key certificates (illustrated in Figures 13-16); authentication using disposable certificates (illustrated in Figures 17-19); authentication using unsigned certificates (illustrated in Figures 20-21); and authentication without certificates, such as in an ecommerce scenario (illustrated in Figure 22).

For a better understanding of the operation of the PKVA according to the presently claimed invention, the Examiner is referred to the example authentication with traditional public key certificates employing a PKVA which is illustrated in Figures 13-16 and described in the specification at page 27, line 12 through page 35, line 14. As illustrated in Figure 13, a public key infrastructure (PKI) includes a traditional certificate authority (CA) 705, a subject 706, and a verifier 707. In authentication with traditional public key certificates, a subject registers its public key and identity attributes with a traditional certificate authority. The certificate authority verifies that the attributes apply to the subject, then signs a certificate that binds the subject's public key to the attributes. The subject proves it identity to a verifier by submitting the certificate and demonstrating knowledge of its private key associated with the public key contained in the certificate. As further illustrated in Figure 13, PKVA 701 is distinct and separate from traditional CA 705. This is because the PKVA is employed to validate the public key of the subject before a private/public key pair of the subject is used for authentication purposes.

As to the limitations of independent claim 1, the PKVA of claim 1 includes a registration authority which issues a first unsigned public key validation certificate (unsigned PKVC) off-line to a subject that binds a public key of the subject to a first public key serial number (PKVN). The registration authority maintains a certificate database of unsigned PKVCs in which it stores the first unsigned PKVC. A credentials server issues a disposable public key validation certificate (disposable PKVC) on-line to the subject. The disposable

PKVC binds the public key of the subject from the first unsigned PKVC to the first PKVN from the first unsigned PKVC. The credentials server maintains a table that contains entries corresponding to valid unsigned PKVCs stored in the certificate database.

Independent claim 21 includes similar limitations to those of claim 1 in defining a method for managing the validity status of a subject's public key. The method includes issuing off-line to a subject a first unsigned PKVC that binds a public key of the subject to a first PKVN, maintaining a certificate database of unsigned PKVCs in which the first unsigned PKVC is stored, issuing on-line to the subject a disposable PKVC that binds the public key of the subject from the first unsigned PKVC to the first PKVN from the first unsigned PKVC, and maintaining a table that contains entries corresponding to valid unsigned PKVCs stored in the certificate database.

The Ramasubramani et al. patent does not teach or suggest all of the above limitations of independent claims 1 and 21. The Ramasubramani et al. patent at column 7, lines 33-60 discloses:

> It has been described that it takes a noticeable length of time in a regular full-power desktop computer to obtain a certificate from a CA and generate a pair of keys; private and public keys therefor. To minimize the latency of obtaining a certificate with a mobile device, a certificate manager module (CMM) 342 maintains a certificate database, preferably in the database 328, to reserve a list of undesignated but issued certificates, referred to as free certificates, from one or different CAs. Whenever a user account is created to activate a mobile device that requires one or more certificates to access certain web servers requiring a certificate, a certificate request (certRequest) signal is sent to the CMM 342 to fetch needed certificates from the certificate database. Upon receiving the fetched certificates from the certificate database, the CMM 342 assigns the certificates to the particular account by attaching the device ID 316 and other account information, hence the fetched certificates become associated to the particular account and are placed in the certificate list 320. Meanwhile the CMM examines the number of the free certificates available in the certificate database, if the number is below a value, for example 200 certificates, referred to as threshold, the CMM calls the HTTP module 330 to establish a connection to the appropriate CA via the landnet 104 to obtain new free certificates to fill up the certificate database till the level of the threshold is reached, as such there are always sufficient free certificates available in the certificate database to supply any new accounts with the ready-to-use free certificates.

Thus, the Ramasubramani et al. patent disclosed CMM 342 contains a database of a list of undesignated but issued certificates referred to as free certificates to minimize latency of obtaining a certificate with a mobile device. Operating based on a threshold, the CMM obtains new free certificates to fill up the certificate database until the level of the threshold is reached, such that there are always sufficient free certificates available in the certificate database to supply any new accounts with the ready-to-use free certificates. Therefore, the undesignated certificates contained in the certificate database by CMM 342 are similar to the certificates signed by traditional certificate authority 705 in the embodiment of the present invention illustrated in Figure 13. Consequently, these undesignated issue certificates are in no way equivalent to the unsigned public key validation certificate (unsigned PKVC) issued offline in the limitations of claims 1 and 21.

In addition, the device ID 316 and other account information disclosed in the above passage of the Ramasubramani et al. patent are not equivalent to the public key serial number (PKVN) recited in independent claims 1 and 21.

Moreover, the Examiner cites the certificate database obtained by CMM 342 in the Ramasubramani et al. patent both for the limitation of the registration authority maintaining a certificate database of unsigned PKVCs in which it stores the first unsigned PKVC and for the table maintained by the credential server that contains entries corresponding to valid unsigned PKVCs stored in a certificate database. The certificate database maintained by CMM 342 in the Ramasubramani et al. patent cannot be both the certificate database of claims 1 and 21 and the table of claims 1 and 21 that contains entries corresponding to valid unsigned PKVCs stored in the certificate database.

In addition, the Examiner asserts that the certificate request (certRequest) signal being sent to the CMM 342 to fetch needed certificates from the certificate database in the Ramasubramani et al. patent teaches the on-line credential server for issuing a disposable public key validation certificate (disposable PKVC) on-line to the subject. As discussed above, however, CMM 342 issues free certificates to minimize the latency of obtaining a certificate with a mobile device and the free certificates are in no way equivalent to a disposable public key validation certificate as recited in independent claims 1 and 21.

Thus, the Ramasubramani et al. patent does not teach or suggest all of the limitations of independent claims 1 and 21. Furthermore, dependent claims 2-8, 10, 14, and 17-20

further define patentably distinct independent claim 1, and dependent claims 22-28 and 30 further define patentably distinct independent claim 21. Therefore, these dependent claims are also believed to be allowable.

Therefore, applicant respectfully requests that the rejections to claims 1-8, 10, 14, 17-28, and 30 under 35 U.S.C. § 102 based on the Ramasubramani et al. patent be withdrawn and these claims be allowed.

The Examiner rejected claims 37-47 and 49-59 under 35 U.S.C. § 102 (e) as being anticipated by the Perlman et al. U.S. Patent 6,230,266.

As discussed above, the subject matter claimed in the pending claims relates to a subject employing a public key validation service (PKVS) to validate the subject's public key before using the public/private key pair for authentication purposes, in such a way that the public key will cease to be usable for authentication purposes if the subject notifies the PKVS that the private key has been compromised. The PKVS includes one or more public key validation agents (PKVAs), each PKVA having a private/public key pair for a digital signature cryptosystem. In embodiments of the present invention, the subject may use its private/"validated" public key pair for multiple authentication purposes. In the example authentication with traditional public key certificates employing a PKVA illustrated in Figures 13-16, a public key infrastructure (PKI) includes a traditional certificate authority (CA) 705, a subject 706, and a verifier 707. PKVA 701 is distinct and separate from traditional CA 705. This is because the PKVA is employed to validate the public key of the subject before a private/public key pair of the subject is used for authentication purposes.

The PKI of independent claim 37 includes a first PKVA configured to maintain a record representing the status of validity of the subject's public key. The record has a high probability of being different from all other records of the first PKVA or of any other PKVA. The PKI of independent claim 37 also includes a verifier configured to respond to an authentication of the subject. The authentication includes ascertaining the validity of the subject's public key according to the record of the first PKVA.

The Perlman et al. patent does not teach or suggest all of the above limitations of independent claim 37. The Examiner asserts that passages of the background of the Perlman et al. patent which discuss a traditional certificate authority (CA) teach the limitations of claim 37 of a first PKVA configured to maintain a record representing the status of validity of

the subject's public key, and wherein the record has a high probability of being different from all other records of the first PKVA or of any other PKVA. By definition, the PKVA of claim 37 must be distinct and separate from any certificate authority.

In addition, the PKVA of claim 37 maintains a record representing the status of validity of the subject's public key which is in not equivalent to the traditional CA of the Perlman et al. patent generating identity certificates. As stated in the Perlman patent, the CA is used to "know which public key belongs to which principal" (Column 1, lines 65-66) and to verify "the relationship between the public key and the principal to which it belongs" (Column 2, lines 6-7). By contrast, as defined in claim 37, the PKVA maintains a record representing the status of validity of the subject's public key and the authentication by the verifier includes ascertaining the validity of the subject's public key according to the record of the first PKVA.

The Examiner also asserts that passages of the background of the Perlman et al. patent discussing an on-line revocation server (OLRS) that maintains a database of certification revocation status information teaches the limitations of claims 37 of a verifier configured to respond to an authentication of the subject, wherein the authentication includes ascertaining the validity of the subject's public key according to the record of the first PKVA. Applicant respectfully notes that the OLRS disclosed in the Perlman et al. patent is similar to the on-line certificate status protocol (OCSP) disclosed in the Background of the Invention section of the Present Application, at page 4, lines 3-12, which operates to permit the verifier of the public key certificate to ask the certificate authority if the certificate is currently valid. The operation of the OLRS disclosed in the Perlman et al. patent and the OCSP disclosed in Present Application which facilitate determining if the certificate is valid are not equivalent to the authentication by the verifier including ascertaining the validity of the subject's public key according to the record of the first PKVA as recited in claim 37.

In view of the above, the Perlman et al. patent does not teach or suggest independent claim 37. Furthermore, dependent claims 38-47 and 49-59 further define patentably distinct independent claim 37. Therefore, these dependent claims are also believed to be allowable.

Therefore, applicant respectfully requests that the rejections to claims 37-47 and 49-59 under 35 U.S.C. § 102 (e) based on the Perlman et al. patent be withdrawn and these claims be allowed.

Claim Rejections under 35 U.S.C. § 103

The Examiner rejected claims 9, 11-13, 16, 29, 31-33, and 36 as being unpatentable over the Ramasubramani et al. patent in view of the Andrews et al. U.S. Patent No. 6,324,645.

In view of the above, the Ramasubramani et al. patent does not teach or suggest all of the limitations of independent claims 1 and 21. Dependent claims 9, 11-13, and 16 further define patentably distinct independent claim 1. Dependent claims 29, 31-33, and 36 further define patentably distinct independent claim 21. Therefore, these dependent claims are also believed to be allowable.

Therefore, applicants respectfully request that the rejections to claims 9, 11-13, 16, 29, 31-33, and 36 based on the combination of the Ramasubramani et al. patent and the Andrews et al. patent be withdrawn and these claims be allowed.

The Examiner rejected claim 48 under 35 U.S.C. § 103 as being unpatentable over the Perlman et al. patent in view of the Andrews et al. patent.

In view of the above, the Perlman et al. patent does not teach or suggest independent claim 37. Dependent claim 48 further defines patentably distinct independent claim 37. Therefore, dependent claim 48 is also believed to be allowable.

Therefore, applicants respectfully request that the rejection to claim 48 under 35 U.S.C. § 103 based on the combination of the Perlman et al. patent and the Andrews et al. patent be withdrawn and claim 48 be allowed.

CONCLUSION

In view of the above, Applicant respectfully submits that pending claims 1-14, 16-34, and 36-59 are in form for allowance and are not taught or suggested by the cited references. Therefore, reconsideration and withdrawal of the rejections and allowance of claims 1-14, 16-34, and 36-59 is respectfully requested.

No fees are required under 37 C.F.R. 1.16(b)(c). However, if such fees are required, the Patent Office is hereby authorized to charge Deposit Account No. 08-2025.

The Examiner is invited to contact the Applicant's representative at the below-listed telephone numbers to facilitate prosecution of this application.

Any inquiry regarding this Amendment and Response should be directed to either Patrick G. Billig at Telephone No. (612) 573-2003, Facsimile No. (612) 573-2005 or William J. Streeter, Esq. at Telephone No. (970) 898-7247, Facsimile No. (970) 898-3886. In addition, all correspondence should continue to be directed to the following address:

Hewlett-Packard Company
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

Respectfully submitted,

Francisco Corella

By his attorneys,

DICKE, BILLIG & CZAJA, PLLC
Fifth Street Towers, Suite 2250
100 South Fifth Street
Minneapolis, MN 55402
Telephone: (612) 573-2003
Facsimile: (612) 573-2005

Date: 12-2-04
PGB:cmj

Patrick G. Billig
Reg. No. 38,080

CERTIFICATE UNDER 37 C.F.R. 1.8: The undersigned hereby certifies that this paper or papers, as described herein, are being deposited in the United States Postal Service, as first class mail, in an envelope address to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on this 2 day of December, 2004.

By
Name: Patrick G. Billig